高等学校本科应用型教材

计算机系统安全

曹天杰　张永平　苏　成

高 等 教 育 出 版 社

内 容 提 要

本书全面系统地介绍了计算机系统安全知识，反映了计算机系统安全领域的新概念、新发展。全书分十三章，涉及了密码学、物理安全、运行安全（风险分析、审计跟踪、备份与恢复、应急）、信息安全（网络安全、访问控制、认证等）等内容。

本书概念准确、选材合理、结构紧凑、条理清晰。书中提供的习题与实验有助于读者进一步深化学习。本书适合计算机科学与技术、信息安全等专业作为“计算机系统安全”、“计算机网络安全”等相关课程的本专科教材，也可作为工程技术人员系统学习信息安全理论的参考书。

前　言

计算机在政治、军事、金融、商业等部门的应用越来越广泛，社会对计算机网络信息系统的依赖也越来越大，安全可靠的网络空间已经成为支撑国民经济、关键性基础设施以及国防的支柱，随着全球安全事件的逐年增多，确保网络信息系统的安全已引起世人的关注，信息安全在各国都受到了前所未有的重视。“9.11”之后，美国联邦调查局所属的关键性基础设施保护中心发布了《关于网络空间安全的国家战略》的报告，明确地将信息安全提升到了关系国家安全的战略高度，“信息安全 + 国土安全 = 国家安全”正逐渐得到社会的认同。

我国正逐步形成一个完善的统一的安全保障体系，成立了国家计算机网络应急处理协调中心（简称 CNCERT，http://www.cert.org.cn/）、国家计算机病毒应急处理中心（http://www.antivirus-china.org.cn/）、国家计算机网络入侵防范中心（http://www.nipc.org.cn/）、信息安全国家重点实验室（http://www.is.ac.cn/）等一批国家级机构。信息安全、信息对抗、密码学等专业已开始在许多高校及科研院所招生，并开设了“计算机系统安全”、“密码学”等相关课程，但目前我国信息安全人才依然缺乏，内容系统全面反映最新进展的优秀本科信息安全教材还不多见。

根据“计算机系统安全”的教学需要，我们从 2000 年开始编写讲义，在多年讲授该课程的基础上，不断充实改进，完成了本教材。

安全的概念是与时俱进的，历经了可靠性、保密、保护，而发展到今天的信息保障。本书从技术的角度介绍了信息安全保障体系，从管理的角度介绍了风险管理，并进一步强调系统安全是一个动态的整体的安全。

本书内容全面、系统，涉及了计算机系统安全的主要方面，如物理安全、运行安全（风险分析、审计跟踪、备份与恢复、应急）、信息安全（网络安全、访问控制、认证等）。全书分十三章：计算机系统安全概述、计算机系统的物理安全、计算机系统的可靠性、密码学基础、消息认证与数字签名、公开密钥基础设施 PKI、身份认证、访问控制、防火墙、攻击与应急响应、入侵检测、IP 安全、安全套接层（SSL）协议。

本书选材合理，结构紧凑。例如作为信息安全基础的密码学，内容十分丰富，1976 年 W. Diffie 和 M. E. Hellman 发表的《密码学的新方向》，以及 1977 年美国公布实施的数据加密标准 DES，标志着密码学发展的革命。2001 年 11 月美国国家标准技术研究所 NIST 发布的高级数据加密标准 AES 代表着密码学的最新

发展。本书以简练的语言涵盖了现代密码学的基本内容，介绍了用于军事、移动通信领域的序列密码，分析了简洁、快速、适于软/硬件加密并且已经标准化的DES、AES等典型分组密码，叙述了适合于数字签名、身份认证、密钥交换等领域的公开密钥密码，并讨论了应用广泛的RSA算法。

本书内容反映了近几年计算机系统安全领域的新发展。如介绍了密码体制的可证明安全、语义安全，介绍了取代DES的美国高级数据加密标准AES、零知识身份证明、基于角色的访问控制RBAC、代理服务技术、IDS的标准化、风险管理与应急响应，等等。

本书参考了大量的RFC文档（http://www.ietf.org/rfc.html）、美国国家标准技术研究所出版物（http://csrc.nist.gov/publications/），也希望读者在学习的过程中查阅参考。

本书适合计算机科学与技术、信息安全等专业本科使用，可以作为“计算机系统安全”、“计算机网络安全”等相关课程的教材，也可以作为工程技术人员系统地学习信息安全理论的参考书。

编者感谢信息安全国家重点实验室的林东岱研究员、南开大学数学科学学院的胡健伟教授和孙澈教授给予的指导。感谢信息安全国家重点实验室的博士后徐涛、博士后黄寄宏、博士生孙海波、硕士生李绪蜂、硕士生孟江涛、中科院数学与系统科学研究所的硕士生程贯中、北京大学数学学院的硕士生魏晋伟等的热情支持，感谢中国矿业大学计算机学院的夏士雄院长、张虹教授、殷兆麟教授，感谢南京大学计算机科学与技术系的黄皓教授、博士生林果园等在本教材的编写过程中给予的各种不同形式的帮助。

信息安全国家重点实验室的薛锐研究员仔细审阅了本书，提出了许多宝贵的意见和建议，编者在此表示特别的感谢。

编者衷心希望读者对本教材批评指正。

曹天杰

于中国科学院软件所信息安全国家重点实验室

2003年6月

目　录

第一章　计算机系统安全概述

! " !　计算机系统安全的概念

! "! "!　世界范围内日益严重的安全问题

ÐÅÏ¢¼¼ÊõºÍ ÐÅÏ¢²úÒµÕýÔÚ¸Ä±ä´«Í³µÄÉú²ú¡¢¾ÓªºÍ Éú»î·½Ê½£¬ÐÅÏ¢ÒÑ³ÉÎª Éç»á·¢Õ¹µÄÖØÒªÕ½ÂÔ×ÊÔ´¡£µç×ÓÉÌÎñ¡¢µç×ÓÕþÎñ¡¢µç×ÓË°Îñ¡¢µç×ÓÒøÐÐ¡¢µç×Ó£¹Ø¡¢µç×ÓÖ¤È¯¡¢ÍøÂçÊéµê¡¢ÍøÉÏÅÄÂô¡¢ÍøÂç¹ºÎï¡¢ÍøÂç·À»¤¡¢ÍøÂçÊ¹ÓÃ #$%¨ #&'()*+, $+-+(.&/0 %/*+1,2*3&/£¬¼ÆËã»úµçÐÅ¼¼ÊõÎ£¨ÍøÂçÊéµê¡¢ÍøÉÏÅÄÂô¡¢ÍøÂç¹ºÎï¡¢ÍøÂç·À»¤£©ÒÔÆäÎÞ·¨¹À¼ÆµÄËÙ¶È·¢Õ¹£¬ÐÅÏ¢¼¼Êõ ÕýÔÚ¸Ä±äÈËÀàµÄÉú»î·½Ê½ºÍ¹¤×÷·½Ê½£¬ÐÅÏ¢°²È«ÎÊÌâÒÑ³ÉÎª Éç»á·¢Õ¹µÄÖØÒª±£ÕÏ¡£

ÔÚ¼ÆËã»úÓ¦ÓÃÈÕÒæÆÕ¼°µÄÍ¬Ê±£¬¼ÆËã»úÍøÂçµÄ°²È«ÎÊÌâ ÈÕÒæÍ»³ö¡£ÍøÂçµÄ¿ª·ÅÐÔ¡¢¹²ÏíÐÔºÍ»¥ÁªÐÔµÈÌØÕ÷£¬´ÓÒ»¿ªÊ¼¾ÍÒþ²Ø×Å²»°²È«µÄÒòËØ£¬ÍøÂçÐÅÏ¢ µÄ°²È«ÎÊÌâÒ²±äµÃÔ½À´Ô½ÖØÒª¡£

!456 Äê³õÔÚ »ùÒ»¹¹ µÄ ÀºÍ ¶û£¨72.&,+£©¸¹Ìý ÌØ£¨8293*£©¹ °¢Ä·½ÏµÄ : ';2<£© Á½ÈËµÄ±àÐ´µÄ=2>39*2/ ²¡ ¶¾£¨8,23/£©ÎÞÒâÖÐ¹«µ½ÁËÊÀ½ç¸÷µØ¡£

!455 Äê!! ÔÂ£¬ÃÀ¹ú¿µÄÎ¶û´óÑ§µÄÑ§Éú ?&,,39 ±àÐ´ÁËÃÀ¹ú Èä³æ¼ÆËã»ú²¡¶¾£¨ ¹ý ÓÃ¢ØÍø´«²¥£¬ÊÂ¹ÊÍøÂçÖÐÔ¼6AAA Ì¨ ¼ÆËã»ú±»´«È¾£¨%/*+,/+* ²» ÄÜÕý³£ÔËÐÐ£©ÔìÉ³É ¾¼ÃËðÊ§Ô¼ ÒÚÃÀÔª¡£ÆÈÊ¹ÃÀ¹ú Õþ®Á¢¼´×é³ö ·´ Ó¦£¬¼ú ·À²¿³ÉÁ¢Á¼ÆËã»úÓ¦¼± ÐÐ¶¯Ð¡×é¡£ÕâÊÇ×»Î ·Ç³£ µäÐÍµÄ¼ÆËã»ú²¡¶¾È¨Ç¿¼ÆËã»úÍøÂçµÄÊÂ¼þ¡£

!446 Äê!B ÔÂB4 ÈÕ£¬ÃÀ¹ú¿ÍÇÖÈëÃÀ¹ú¿Õ¾üµÄ»ÇÆøÍøÖ·²¢½«ÆäÖ÷Ò³ËÁÒâ¶Ä¶¯£¬ÆäÊ¹ÃÀ¹ú¹ú·À²¿Ò»¶ÈÊ¹Ø±ÕÁËÆäËüû5A ¶à¸ö¾üÊÂÍøÕ¾¡£

!445 Äê6 ÔÂ!6 ÈÕ£¬ÃÀ¹ú ÈëÇÖÃÀÊÏ°£Ä³ÐÅÏ¢ÍøµÄ5 Ì¨ ·þÎñÆ÷£¬Æä»áÁËËû Ãç´ ²¿·Ö¹¤×÷ÈËÔ±µÄ¿ÚÁîºÍ CAA ¶à¸ö ºÍ ·¨ ÓÃ»§µÄÕÊºÅ ÃÜÂë£¬ÆäÖÐ¼ü À¨Á½¨ ·þÎñ ÆäËû³¬¼¶ÓÃ»§µÄÕÊºÅ ÃÜÂë¡£

!445 Äê!A ÔÂB@ ÈÕ£¬Ö¸Õ¿ªÍ¨ µÄÓÉÖÐÈ«ÈËÈ¨Ñ§»áÓëÖÐ¹ú¼Ê»¥Áª ÍøÐÅÏ¢ÖÐÐÄ¹ ´´ °ì µÄ ÖÐ¹úÈËÈ¨Ñ§»áÍøÕ¾ÔâµÈ ºÚ¿Í¹¥»÷ÍøÕ¾Ö¸Ä¡£

BAAA ÄêD ÔÂ6 ÈÕ 6 Ê±CA ·Ö£¬ÃÀ¹ú °×¹¬ÍøÕ¾Ôâµ½Ò±»ºÚ¡£

BAA! ÄêÄÏº£×²»úÊÂ¼þÒý¢ÖÐÃÀºÚ¿Í´óÕ½£¬ÖÐÃÀË«·½¸÷ÓÐÊýÇ§ÍøÕ¾±»ºÚ¡£

hacker

hacking

honker

cracker

1.1.2 计算机系统安全的概念

从技术角度看,计算机系统安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。我们首先介绍以下几个概念。

计算机系统(Computer System Computer Information System

Computer System Security

ISO

NII

Availability

些信息或者否认它的内容的企图不能得逞；二是交付证明，它提供给信息发送者以证据，这将使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

除此之外计算机网络信息系统的其他安全属性还包括：

可控性：可控性就是对信息及信息系统实施安全监控。管理机构对危害国家信息的来往、使用加密手段从事非法的通信活动等进行监视审计，对信息的传播及内容具有控制能力。

可审查性：使用审计、监控、防抵赖等安全机制，使得使用者（包括合法用户、攻击者、破坏者、抵赖者）的行为有证可查，并能够对网络出现的安全问题提供调查依据和手段。审计是通过对网络上发生的各种访问情况记录日志，并对日志进行统计分析，是对资源使用情况进行事后分析的有效手段，也是发现和追踪事件的常用措施。审计的主要对象为用户、主机和节点，主要内容为访问的主体、客体、时间和成败情况等。

认证：保证信息使用者和信息服务者都是真实声称者，防止冒充和重演的攻击。

访问控制：保证信息资源不被非授权地使用。访问控制根据主体和客体之间的访问授权关系，对访问过程做出限制。

安全工作的目的就是为了在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，维护计算机系统安全。我们应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。计算机系统安全涉及物理安全（实体安全）、运行安全和信息安全三个方面。

（1）物理安全（Physical Security）

保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。特别是避免由于电磁泄漏产生信息泄露，从而干扰他人或受他人干扰。物理安全包括环境安全，设备安全和媒体安全三个方面。

（2）运行安全（Operation Security）

为保障系统功能的安全实现，提供一套安全措施（如风险分析，审计跟踪，备份与恢复，应急等）来保护信息处理过程的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存贮、处理和传输的信息造成破坏和损失。运行安全包括风险分析、审计跟踪、备份与恢复、应急四个方面。

风险分析是指为了使计算机信息系统能安全地运行，首先了解影响计算机信息系统安全运行的诸多因素和存在的风险，从而进行风险分析，找出克服这些风险的方法。

审计跟踪是利用计算机信息系统所提供的审计跟踪工具,对计算机信息系统的工作过程进行详尽的跟踪记录,同时保存好审计记录和审计日志,并从中发现和及时解决问题,保证计算机信息系统安全可靠地运行。这就要求系统管理员要认真负责,切实保存、维护和管理审计日志。

应急措施和备份恢复应同时考虑。首先要根据所用信息系统的功能特性和灾难特点制定包括应急反应、备份操作、恢复措施三个方面内容的应急计划,一旦发生灾害事件,就可按计划方案最大限度地恢复计算机系统的正常运行。

(3) 信息安全(Information Security)

防止信息财产被故意地或偶然地非授权泄露、更改、破坏或使信息被非法的系统辨识、控制。即确保信息的完整性、保密性、可用性和可控性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别七个方面。

网络信息既有存储于网络节点上的信息资源,即静态信息;又有传播于网络节点间的信息,即动态信息。而这些静态信息和动态信息中有些是开放的,如广告、公共信息等,有些是保密的,如私人间的通信、政府及军事部门、商业机密等。信息根据敏感性可分为以下类别。

非保密的:不需保护。其实例包括出版的年度报告、新闻信件等。

内部使用的:在公司和组织内部不需保护,可任意使用,但不对外。实例包括策略、标准、备忘录和组织内部的电话记录本等。

受限制的:包括那些泄漏后不会损害公司和组织的最高利益的信息。例如客户数据和预算信息等。

保密的:包括那些泄漏后会严重损害公司和组织利益的信息。例如市场策略和专用软件等。保密数据根据其保密程度可分为秘密、机密、绝密三类。敏感性程度依次递增这是按照泄漏后对公司和组织利益的损害程度来排序的。

计算机系统的安全保护工作的重点是维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

我国公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门,在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法,由公安部会同有关部门制定。计算机信息系统的使用单位应当建立健全安全管理制度,负责本单位计算机信息系统的安全保护工作。

1.1.3 国内外计算机系统安全标准

国际性的标准化组织主要有国际标准化组织(ISO)、国际电器技术委员会(IEC)及国际电信联盟(ITU)所属的电信标准化组(ITU – TS)。

美国国防部的可信计算机系统评价准则(Trusted Computer System Evaluation Criteria TCSEC,桔皮书)是计算机系统安全评估的第一个正式标准,具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出,并于 1985 年 12 月由美国国防部公布。TCSEC 将安全分为 4 个方面:安全政策、可说明性、安全保障和文档。该标准将以上 4 个方面分为 7 个安全级别,按安全程度从最低到最高依次是 D、C1、C2、B1、B2、B3、A1。

D 类:最低保护。无需任何安全措施。属于这个级别的操作系统有:DOS、Windows、Apple 的 Macintosh System7.1。

C1 类:自决的安全保护。系统能够把用户和数据隔开,用户可以根据需要采用系统提供的访问控制措施来保护自己的数据,系统中必有一个防止破坏的区域,其中包含安全功能。用户拥有注册帐号和口令,系统通过帐号和口令来识别用户是否合法,并决定用户对程序和信息拥有什么样的访问权。

C2 类:访问控制保护。控制粒度更细使得允许或拒绝任何用户访问单个文件成为可能。系统必须对所有的注册、文件的打开、建立和删除进行记录。审计跟踪必须追踪到每个用户对每个目标的访问。能够达到 C2 级的常见操作系统有:Unix 系统、XENIX、Windows NT。

B1 类:有标签的安全保护。系统中的每个对象都有一个敏感性标签而每个用户都有一个许可级别。许可级别定义了用户可处理的敏感性标签。系统中的每个文件都按内容分类并标有敏感性标签,任何对用户许可级别和成员分类的更改都受到严格控制。较流行的 B1 级操作系统是 OSF/1。

B2 类:结构化保护。系统的设计和实现要经过彻底的测试和审查。系统应结构化为明确而独立的模块,实施最少特权原则。必须对所有目标和实体实施访问控制。政策要有专职人员负责实施,要进行隐蔽信道分析。系统必须维护一个保护域,保护系统的完整性,防止外部干扰。目前,UnixWare 2.1/ES 作为国内独立开发的具有自主版权的高安全性 Unix 系统,其安全等级为 B2 级。

B3 类:安全域。系统的安全功能足够小,以利广泛测试。必须满足参考监视器需求以传递所有的主体到客体的访问。要有安全管理员,审计机制扩展到用信号通知安全相关事件,还要有恢复规程,系统高度抗侵扰。

A1 类:核实保护。最初设计系统就充分考虑安全性。有“正式安全策略模型”,其中包括由公理组成的数学证明。系统的顶级技术规格必须与模型相对应,系统还包括分发控制和隐蔽信道分析。

1991 年,欧共体发布了信息技术安全评价准则(Information Technology Security Evaluation Criteria,ITSEC)。1993 年,加拿大发布了加拿大可信计算机产品评价准则(CTCPEC),CTCPEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年,美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上,发布了美国信息技术安全评价联邦准则(FC)。ITSEC 与 TCSEC 不同,其观点是应当分别衡量安全的功能和安全的保障,而不应象 TCSEC 那样混合考虑安全的功能和安全的保障。因此,ITSEC 对每个系统赋予两种等级:"F"(functionality)即安全功能等级,"E"(European assurance)即安全保障等级。另外,TCSEC 把保密作为安全的重点,而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。CTCPEC 标准将安全需求分为 4 个层次:机密性、完整性、可靠性和可说明性。FC 参照了 CTCPEC 及 TCSEC,在美国的政府、民间和商业领域得到广泛应用。1993 年 6 月,上述国家共同起草了一份通用准则(CC),并将 CC 推广为国际标准。1999 年 10 月 CC v2.1 版发布,并且成为 ISO 标准。CC 结合了 FC 及 ITSEC 的主要特征,它强调将安全的功能与保障分离,并将功能需求分为 9 类 63 族,将保障分为 7 类 29 族。

ISO 在安全体系结构方面制定了国际标准 ISO7498 – 2 – 1989《信息处理系统开放系统互连基本参考模型第 2 部分安全体系结构》。该标准提供了安全服务与有关机制的一般描述,确定在参考模型内部可以提供这些服务与机制的位置。

国内由公安部主持制定、国家技术标准局发布的国家标准 GB17895 – 1999《计算机信息系统安全保护等级划分准则》。该准则将信息系统安全分为 5 个等级,分别是:自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等,这些指标涵盖了不同级别的安全要求。我国红旗安全操作系统 2.0 已通过中华人民共和国公安部计算机信息系统产品质量监督检验中心的认证,达到信息安全第三级的要求。

1.2 安全威胁

1.2.1 安全威胁的种类

安全威胁是指对安全的一种潜在的侵害。威胁的实施称为攻击。一般认为,目前计算机系统安全面临的威胁主要表现在三类:信息泄露、拒绝服务、信息破坏。其中信息泄露、信息破坏也可能造成系统拒绝服务。

信息泄漏:指敏感数据在有意或无意中被泄漏出去或丢失,它通常包括:信

息在传输中丢失或泄漏(如利用电磁泄漏或搭线窃听等方式可截获机密信息,或通过对信息流向、流量、通信频度和长度等参数的分析,推出有用信息);信息在存储介质中丢失或泄漏;通过建立隐蔽隧道等窃取敏感信息等。

信息破坏:以非法手段窃得对数据的使用权,删除、修改、插入或重发某些重要信息,以取得有益于攻击者的响应;恶意添加,修改数据,以干扰用户的正常使用。

拒绝服务:它不断对网络服务系统进行干扰,改变其正常的作业流程,执行无关程序使系统响应减慢甚至瘫痪,影响正常用户的使用,甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

安全威胁可能来自各方面。影响、危害计算机系统安全的因素分自然和人为两类。

自然因素包括:各种自然灾害,如水、火、雷、电、风暴、烟尘、虫害、鼠害、海啸和地震等;系统的环境和场地条件,如温度、湿度、电源、地线和其他防护设施不良造成的威胁;电磁辐射和电磁干扰的威胁;硬件设备自然老化,可靠性下降的威胁。

人为因素又有无意和故意之分。无意事件包括:操作失误(操作不当、误用媒体、设置错误)、意外损失(电力线搭接、电火花干扰)、编程缺陷(经验不足、检查漏项、不兼容文件)、意外丢失(被盗、被非法复制、丢失媒体)、管理不善(维护不利、管理松驰)、无意破坏(无意损坏、意外删除等)。人为故意的破坏包括:敌对势力、各种计算机犯罪。

1. 从威胁的来源看可分为内部威胁和外部威胁

造成网络安全的威胁的原因可能是多方面的,有来自外部,也有可能来自企业网络内部。

内部威胁。80%的计算机犯罪都和系统安全遭受损害的内部攻击有密切的关系。内部人员对机构的运作、结构熟悉,导致攻击不易被发觉,内部人员最容易接触敏感信息,危害的往往是机构最核心的数据、资源等。各机构的信息安全保护措施一般是"防外不防内"。能用来防止内部威胁的保护方法包括:对工作人员进行仔细审查;制订完善的安全策略;增强访问控制系统;审计跟踪以提高检测出这种攻击的可能性。

外部威胁。外部威胁的实施也称远程攻击。外部攻击可以使用的办法如:搭线;截取辐射;冒充为系统的授权用户,或冒充为系统的组成部分;为鉴别或访问控制机制设置旁路;利用系统漏洞攻击等。

2. 从造成的结果上看可以分成主动威胁和被动威胁

被动威胁。这种威胁对信息的非授权泄露而未改变系统状态。如信息窃

取、密码破译、信息流量分析等。被动威胁的实现不会导致对系统中所含信息的任何篡改,而且系统的操作与状态也不受改变,但有用的信息可能被盗窃并被用于非法目的。使用消极的搭线窃听办法以观察在通信线路上传送的信息就是被动威胁的一种实现。

主动威胁。这种威胁是对系统的状态进行故意的非授权的改变。对系统的主动威胁涉及到系统中所含信息的篡改,或对系统的状态或操作的改变。一个非授权的用户不怀好意地改动路由选择表就是主动威胁的一个例子。与安全有关的主动威胁的例子可能是:入侵、篡改消息、重发消息、插入伪消息、重放、阻塞、抵赖、病毒、冒充已授权实体以及服务拒绝等。主动攻击会直接进入信息系统内部,往往可影响系统的运行,造成巨大的损失,并给信息网络带来灾难性的后果。

3. 从威胁的动机上看分为偶发性威胁与故意性威胁

偶发性威胁。偶发性威胁是指那些不带预谋企图的威胁。偶发性威胁的实例包括自然灾害、系统故障、操作失误和软件出错。人为的无意失误包括:操作员安全配置不当造成的安全漏洞,用户安全意识不强,用户口令选择不慎,用户将自己的帐号随意转借他人或与别人共享等都会对网络安全带来威胁。

故意性威胁。故意性威胁是指对计算机系统的有意图、有目的的威胁。范围可从使用易行的监视工具进行随意的检测到使用特别的系统知识进行精心的攻击。一种故意的威胁如果实现就可认为是一种"攻击"。人为的恶意攻击:这是计算机网络所面临的最大威胁,敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种:一种是主动攻击,它以各种方式有选择地破坏信息的有效性和完整性;另一类是被动攻击,它是在不影响网络正常工作的情况下,进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害,并导致机密数据的泄漏。由于网络软件不可能是百分之百的无缺陷和无漏洞的,这些漏洞和缺陷恰恰是攻击者进行攻击的首选目标。

4. 从威胁的严重性可分为三级

C 级威胁。个体单点攻击,攻击的范围、深度和能够完成的攻击任务不太复杂,往往是黑客行为,虽然这种攻击可以逐步实施自动化、平台化,但攻击点是一点,作用有限,通常攻击的是标准化网络和系统。

B 级威胁。有组织分布式协同攻击。多点、多技术和协同攻击,相互掩护,危害大,难于对付。已经采用多种网络攻击技术。能够攻击一些专用网络,非标准网络,攻击软件本身并没有组织化,较少实施或不能实施战术。

A 级威胁。信息战是指通过一切手段(可控计算机病毒、信息炸弹、远程攻击软件、网络攻击平台、使用多技术体制的网络、使用包括卫星通信在内的一切